Information Systems Education Journal (ISEDJ) 11 (2)
ISSN: 1545-679X April 2013

Building a Cybersecurity Workforce with Remote Labs

Nancy Martin
nlmartin@siu.edu

Belle Woodward
bellew@siu.edu

Information Systems Technologies
Southern Illinois University
Carbondale, IL 62901, USA

Abstract

Now more than ever, cybersecurity professionals are in demand and the trend is not expected to change anytime soon. Currently, only a small number of educational programs are funded and equipped to educate cybersecurity professionals and those few programs cannot train a workforce of thousands in a relatively short period of time. Moreover, not only are additional educational resources needed, but the programs need to deliver high quality, hands-on learning for future cybersecurity professionals. Survey results show that lack of funding and lack of equipment prevent some educational institutions from providing a hands-on learning component in security curricula. One solution is the use of remote labs to increase the number of students with access to security lab environments. We propose that it is an appropriate time for Centers of Academic Excellence in Information Assurance and other organizations to collaborate to assist universities, community colleges and even high schools, through the development of remote security labs, to increase our nation's capacity to adequately train a large number of cybersecurity professionals. The authors have recently implemented a remote lab infrastructure to begin testing the viability of the concept on a small scale.

Keywords: cybersecurity, remote lab, hands-on learning, curriculum

1. INTRODUCTION

I hear and I forget
I see and I remember
I do and I understand
Chinese Proverb

Cybersecurity is a serious challenge to all organizations, but especially to governments. The urgency of confronting the challenge increases daily, even exponentially with recent discovery of the Stuxnet worm. The concern was addressed at the federal level in 2009 when our national cybersecurity strategy was updated to include 12 key initiatives. Of key interest to information systems academicians is Initiative #8 of The Comprehensive National Cybersecurity Initiative (CNCI) (National Security Council, 2009) which is the directive to expand cyber education. The need is outlined in the CNCI as follows "…there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field" (p. 4). This urgent need is echoed in the Bureau of Labor

Statistics' Occupational Outlook Handbook. The BLS projects that jobs for network and computer systems administrators will increase by nearly 79,000 from 2008 to 2018. While not all new jobs in this area will require a specialty in security, the BLS notes that "[a]s cyber attacks become more sophisticated; demand will increase for workers with security skills" (U.S. Department of Labor, Bureau of Labor Statistics, 2010-2011). The BLS does not yet identify cybersecurity as a separate job title. However, the National Initiative for Cybersecurity Education (NICE) is addressing this absence of a common language to discuss the work and skill requirements of cybersecurity professionals (National Initiave for Cybersecurity Education, 2011). This absence hinders the ability to identify skill gaps in the security workforce. Nevertheless, it is widely accepted the need for cybersecurity professionals is great and the trend is expected to continue. For example, within the government sector, the Department of Homeland Security alone is expected to hire up to 1,000 cybersecurity professionals over the next three years ("Cyber help wanted," 2009).

The CNCI also expresses concern about the current ability to train cybersecurity personnel: "Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950's, to meet this challenge" (p. 4).

Currently, the U.S. may not be in a position to quickly and adequately train the sizeable cybersecurity workforce needed (Locasto, Ghosh, Jajodia, & Stavrou, 2011). A crucial element of the security professional's job is the ability to analyze and understand a variety of risks and then to evaluate appropriate preventative or responsive measures. Therefore, not only do we need large numbers of cybersecurity professionals, we need them trained in an environment where they can practice these important skills. As Locasto and colleagues (2011) point out, only a small number of educational programs are currently funded and equipped to educate cybersecurity professionals and those few programs cannot train a workforce of thousands in a relatively short period of time. Moreover, not only are additional educational resources needed, but the programs need to deliver high quality, hands-on learning for future cybersecurity professionals.

In this paper, we report on survey results that align with the concern that the U.S. may not be adequately equipped to train large numbers of cybersecurity professionals. In response to the findings, we then suggest a coordinated effort to aid in such training, namely through remote labs. The rest of the paper is laid out as follows: next is a brief literature review supporting hands-on learning; then the findings of the survey are presented as the current state of security curricula; then a brief rationale for a remote lab solution is offered; and finally other considerations and a conclusion are presented.

2. HANDS-ON LEARNING

The traditional method of university learning is through reading (or summarizing) a textbook and doing problems or examples through rote memory of either formula or fact. Hands-on experiences are often used only to verify the facts stated in the textbook (Bork, 2000). In today's environment, educators in all areas of information technology are being challenged to move beyond traditional methods of instruction (i.e. the lecture mode) to an approach that calls for an increased interactivity with students about both the subject content and learning strategies (Bork, 2000). Many educators stress the importance of active learning (Boggs, 1999; Bonwell & Sutherland, 1996; Conklin, 2006; Felder & Brent, 2003), even dating back to Dewey's "genuine education" (Dewey, 1938). It is well accepted among most faculty that a hands-on approach to learning is the preferred method.

Specific to cybersecurity, an integral piece of any training is the opportunity to work in an interactive hands-on environment. Problem solving skills are best developed in this fashion. The incorporation of real world problems needs to include challenges that rise above simplistic scenarios. Instead, these problems need to propel students into the realms of higher order critical thinking skills: analysis, synthesis and evaluation (Bloom, 1956) such as are required in the cybersecurity professional's daily job. Students must be able to practice "professional artistry" (Schön, 1987) in order to prepare for today's cybersecurity career. Problems faced in the daily duties require the professional to look at security issues from both the attack and

defend perspectives, and to adapt to ever changing threats. Therefore, a hands-on curriculum is likely to produce the most effective results in training cybersecurity professionals.
Building upon the theoretical foundation that supports not only collaborative, but also active or hands-on learning, we had the opportunity to redesign our own security curriculum in 2006. All courses in the curriculum hence consist of lecture and lab, with an emphasis on hands-on experience (Woodward & Young, 2007). Outcomes were measured as positive when students placed first of seven teams in their first Regional Collegiate Cyber Defense Competition. Graduates of this curriculum are highly recruited into a variety of information security jobs, and the university is a National Center of Academic Excellence in Information Assurance Education (CAE/IAE).

As a step toward building a national cybersecurity workforce, now is an appropriate time for CAEs to collaborate at a higher level to address the challenge. Given our experience and the experience and capabilities of other CAEs, a suitable approach would be to assist other universities, community colleges and even high schools to "build educational capacity" as first suggested by Locasto and colleagues (Locasto et al., 2011).

Before proceeding however, it is important to consider the current state of cybersecurity curricula.

3. STATE OF CYBERSECURITY HANDS-ON CURRICULUM

Supported by educational theory, we believe that the hands-on component in the security curriculum is the key to student success. Several courses commonly comprise a security curriculum including topics in security awareness, information assurance, network security, forensics, wireless security, and generally, a capstone course. Interestingly, some U.S. educational institutions offer security related courses without a hands-on component.

To better understand the state of security curricula, the authors collected data from a survey administered to security instructors over a six year period, ending in 2011. The survey was distributed to attendees of The Center for Systems Security and Information Assurance Train-the-Trainer courses at a Midwestern location. One hundred thirty-nine instructors responded to survey questions regarding their respective security curricula. The respondents represented 32 universities, 85 community colleges, 8 vocational/technical schools, and 14 high schools. Providing specific demographic data was optional, but at least 20 states were represented from Hawaii to New York and Florida.

Table 1 displays the statistics of greatest concern from the survey: courses offered without a hands-on lab component. The N for universities and community colleges are smaller due to missing responses.

Table 1. Percentage of organizations NOT offering a hands-on component.

N	25	73	8	14
	University	Comm College	Voc/Tech	High School
Sec Awareness	55%	16%	20%	43%
IA I	30%	13%	40%	80%
IA II	56%	23%	60%	100%
Net Sec I	21%	9%	0%	14%
Net Sec II	50%	21%	50%	50%
Forensics I	33%	32%	60%	83%
Forensics II	62%	49%	60%	100%
Wireless Sec	55%	28%	43%	33%
Capstone	50%	31%	60%	57%

Included in the 139 respondents were a number of schools that are designated Centers of Academic Excellence or were in the process of becoming a CAE. The breakdown is displayed in Table 2. Two year colleges are eligible to receive the CAE2Y designation.

Table 2. Number of CAEs by organization type.

	N	CAE	In Progress	% of total
University	32	11	2	40.6%
Comm College	85	10	2	14.1%
Voc/Tech	8	1	0	12.5%

Community college CAEs and the single Vocational/Technical School CAE reported hands-on lab components for all security courses. However, surprisingly, survey results indicated that a number of university level CAEs did not offer hands-on lab components to some courses as shown in Figure 1. Depending on the course, the percentage of university CAEs not offering hands-on components ranged from 33% (Network Security I) to 80% (Forensics II).

For all educational institutions, when asked what barriers prevented the provision of hands-on lab components to the curriculum, lack of funding topped the list. Respondents were allowed to check as many as applied. All barriers are shown in the Table 3.

Figure 1. Percentage of university CAEs NOT offering a hands-on component.

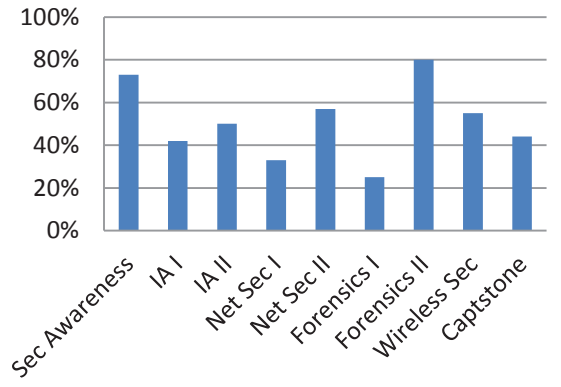

Table 3. Frequency of barriers to providing labs

Barrier	Frequency
Lack of funding	79
Lack of equipment	65
Lack of instructor training	49
Lack of space for equipment	34
Lack of tech support	34
Perceived security vulnerabilities by IT staff	32
Lack of space for student access	27
Lack of training for maintaining equipment	27
Perceived security vulnerabilities by admin	20
Other barriers	20
No barriers	9

The top two barriers, lack of funding and equipment, come as no surprise. In times of economic hardship, education funding is usually at the top of the list for cuts, and it becomes extremely difficult, if not impossible, to secure money for new programs, faculty, and lab equipment. The next three barriers, lack of instructor training, lack of space, and lack of technical support, can also be traced back to funding. Qualified instructors could be hired or current instructors could attend train-the-trainer workshops if funding was available. Space required for equipment and labs could be constructed if training cybersecurity professionals was deemed an urgent need. Likewise, technical support staff could be added or contracted with adequate funding.

The results provide some insight into the issue, but regardless of the reasons, the considerable lack of hand-on training in security curricula, even in some that are designated CAEs, is cause for concern. Considering the growing demand for skilled cybersecurity professionals, we must find ways to get hands-on skills to a large number of individuals, and to do it rather quickly. To that end, we support Locasto et al.'s (2011) suggestion that a collaborative effort among universities, community colleges and high schools is necessary and we argue that the need is urgent.

4. REMOTE LABS AS A SOLUTION

One avenue of collaboration is to offer remote lab access to enrich existing security curricula or to enable security courses to be offered with a lab component even at the high school level. Like traditional labs, remote labs utilize equipment and space, however, the equipment is accessed through a geographically distant computer. However, users are accessing a physical network environment. Remote labs are not to be confused with simulators which provide an emulation of the network environment. Simulators do not always process unexpected or incorrect commands appropriately leaving the user without important information that would have been provided in a physical network environment. Therefore, a simulation does not offer the ability to develop "professional artistry" like a remote lab.

Remote labs offer a number of other advantages as well. Lack of financial resources and equipment top the list of barriers to hands-on labs, but remote labs could be housed in CAEs and funded to provide access to other universities, community colleges, and high schools. Although a degree of funding is required, it would be far less expensive to outfit a number of CAE hubs than to support dozens or hundreds of separate institutions.

Other barriers such as lack of training and lack of support would also be addressed by remote

labs. Training for instructors could be accommodated in the remote lab environment and the technical support would be provided by the CAE hub. On-site workshops and courses could also be provided to other types of organizations such as in the private sector.

Remote labs also afford the opportunity to work in a team environment. Through proper lab settings, students can work on the same network environment simultaneously as part of a team. Additionally, remote labs remove the time and space limitations of traditional labs, thereby allowing more users overall to share the resources. Virtualization software can also help ease the burden of single use network equipment and has been shown to be a viable solution (Wu, 2010).

Not only is the infrastructure barrier addressable with a remote lab environment, but the lab content could be provided as well. The National Security Agency funded SEED project has produced a number of security education labs as well as support material for instructors (Du, 2011). This project could easily be incorporated into a larger remote lab project.

We need a large cybersecurity workforce, and we need one that is hands-on trained in the latest tools and techniques of the field. In the short term, rather than reinventing the wheel in educational organizations across the nation, we should utilize our CAEs to become the hubs of cybersecurity education and training, connecting not only with other educational institutions, but with industry partners as well. Services offered through the CAE hubs could include train-the-trainer workshops, remote access labs, lab content, and even hosting of security colloquia.

The authors recently received local funding to purchase remote lab software and hardware in order to enhance and expand the course offerings within the department and across other campus courses that employ hands-on labs based on desktop computing resources. The technology allows for students to remotely access a wide range of hardware and software resources for use in conjunction with security and networking courses. The technology provides students anywhere, anytime access to lab resources via a standard web browser. Security concerns are also reduced for the host due to the web browser interface. It also provides very powerful and flexible management capabilities for instructors and access to a plethora of industry validated training, learning materials and activities. This is specifically the type of remote lab environment that can be expanded to partner universities, community colleges and even high schools that are burdened by the barriers mentioned in this study.

5. OTHER CONSIDERATIONS

Pushing cybersecurity training down to the high school level is also an important endeavor. Recruiting students into science, technology, engineering and mathematics (STEM) remains a high priority for the U.S. Today's students have grown up in the media age, and little attention to what that means in terms of lifestyle has been introduced into public school curricula. For example, issues such as the need to focus on personal privacy and avoidance of intellectual property violations should be standard discourse in public schools. There is great need to initiate these conversations at an early age, and to expose students to the idea of cybersecurity. Providing workshops and hands-on lab access could aid in that type of training. Barring full scale cybersecurity curricula or courses in high schools, even offering workshops or in-class demonstrations could fuel interest in the STEM fields, and particularly in cybersecurity. These platforms could serve as recruiting tools for all students, including minorities, and women to fulfill skill needs of the future workforce. Recruiting more students into computing and technology disciplines will likely result in more students choosing cybersecurity as a profession.

In the longer term, standard curricula should be embraced by universities, community colleges, and even high schools. The ITiCSE Information Assurance Curriculum Guidelines Working Group has published preliminary guidelines for security curriculum (Cooper et al., 2010). The final document is expected to be published as IA2013. The guide will provide knowledge areas and specific subjects that are recommended for a security curriculum. While the guide does not specifically address hands-on learning in the body of knowledge, the authors certainly recognize its value: "[the] working group considers such practical hands-on training as important means that can be used to reach the learning goals…" (Cooper et al., 2010).

6. CONCLUSION

U.S. organizations, both government and private, need a massive, well-trained cybersecurity workforce sooner rather than later. The infrastructure to train small numbers is there. Funding remote labs to expand capacity is a timely idea that could address the demand relatively quickly and economically. It is through the remote lab environment that students will gain the hands-on experience component deemed vital by educational theorists. This will lead to effective education and training which enables our country to build the specialized workforce with the right skills, at the right time and place to protect our citizens and assets. Although the use of remote labs is not a new idea, the authors have now put the infrastructure in place to test the viability of the solution. The next step is to analyze the opportunities now available through our own remote lab software. Effort is underway to plan an initial slate of offerings across our campus and with partner schools. Future research will follow the progress of these efforts.

7. REFERENCES

Bloom, B. (1956). *Taxonomy of educational objectives, handbook I: The cognitive domain*. New York: David McKay Company, Inc.

Boggs, G. (1999). What the learning paradigm means for faculty. *New Directions for Teaching and Learning*, *51*(5), 3–5.

Bonwell, C., & Sutherland, T. (1996). The active learning continuum: Choosing activities to engage students in the classroom. In T. Sutherland & C. Bonwell (Eds.), (pp. 3–16). San Francisco: Jossey-Bass, Inc.

Bork, A. (2000). Learning technology. *Educause Review*, *35*(1), 74–81.

Conklin, A. (2006). Cyber defense competition and information security education: An active learning solution for a capstone course. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*. Kauai, HI.

Cooper, Nickell, C., Perez, L., Oldfield, B., Brynielsson, J., Gokce, A., Hawthorne, E., et al. (2010). Towards information assurance (IA) curricular guidelines. *Proceedings of the 2010 ITiCSE Working Group Reports* (pp. 49–64). Presented at the ITiCSE-WGR '10, Ankara, Turkey: ACM.

Cyber help wanted [Editorial]. (2009, August 1).*Washington Post*.

Dewey, J. (1938). *Experience and education*. New York: Touchstone Book, Simon & Schuster, Inc.

Du, W. (2011). Developing instructional laboratories for computer SEcurity EDucation. Retrieved from http://www.cis.syr.edu/~wedu/seed/

Felder, R., & Brent, R. (2003). Learning by doing. *Chemical Engineering and Education*, *37*(4), 282–283.

Locasto, M., Ghosh, A., Jajodia, S., & Stavrou, A. (2011). The ephemeral legion: producing an expert cyber-security work force from thin air. *Communications of the ACM*, *54*(1), 129–131.

National Initiative for Cybersecurity Education. (2011). *Cybersecurity workforce framework*.

National Security Council. (2009). *The comprehensive national cybersecurity initiative*.

Schön, D. (1987). *Educating the reflective practitioner*. San Francisco: John Wiley & Sons, Inc.

Woodward, B., & Young, T. (2007). Redesigning an information security curriculum through application of traditional pedagogy and modern business trends. *Information Systems Educators Journal*, *5*(11), 3–11.

Wu, Y. (2010). Benefits of virtualization in security lab design. *ACM Inroads*, *1*(4), 38–42.